



Privacy Act of 1974; System of Records

AGENCY: Veterans Benefits Administration, Department of Veterans Affairs (VA).

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is modifying the system of records entitled, “Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA” (138VA005Q), by updating the routine uses and by adding routine use 13. This system of records is an electronic repository of military personnel’s military history, payroll information and their dependents’ data provided to VA by the Department of Defense’s Defense Manpower Data Center (DMDC). The VADIR database repository is used in conjunction with other applications across VA business lines to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and Department of Defense (DoD). VA applications use the VADIR database to retrieve profile data, as well as address, military history, and information on compensation and benefits, disabilities, and dependents.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the *Federal Register*. If no public comment is received during the period allowed for comment or unless otherwise published in the *Federal Register* by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the *Federal Register*. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW, (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to “Veterans

Affairs/Department of Defense Identity Repository (VADIR)-VA" (138VA005Q).

Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: James Whited, Director, Technical Integration, 1615 Woodward St, Austin, TX 78741, phone 512-326-6302, james.whited@va.gov.

SUPPLEMENTARY INFORMATION: VA has updated the routine uses and descriptions. The amended system of records reflects the updates to the routine uses. Additionally, routine use number 13 is added. This routine use allows VA to enter into Computer Match Agreements (CMAs) with other Federal agencies to determine or verify eligibility of veterans receiving VA benefits or medical care under title 38, U.S.C. No significant alterations have been made to the types, numbers, maintenance or organization of records or to the purpose or procedures for maintaining the information. In accordance with 5 U.S.C. 552a(r), the notice of intent to publish and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director, Office of Management and Budget.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Kurt D. DelBene, Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on December 13, 2022 for publication.

Dated: December 20, 2022.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA (138VA005Q).

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Austin Information Technology Center, 1615 East Woodward Street, Austin, Texas 78772.

SYSTEM MANAGER(S): Alexander Torres, Project Manager, 812 Gilardi Dr Petaluma, CA 94952, phone (703) 300-5511, Alexander.Torres@va.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The authority for maintaining this system is title 38 U.S.C. section 5106.

PURPOSE(S) OF THE SYSTEM: The purpose of VADIR is to receive electronically military personnel and payroll information from the Department of Defense (DoD) in a centralized VA system and then distribute the data to other VA systems and lines of business who require the information for health and benefits eligibility determinations. This information is provided to VADIR by the Defense Manpower Data Center (DMDC). VADIR will also provide veterans information concerning education benefits usage and death and disability status, as well as personal and demographic information on veterans discharged prior to 1978 to DMDC for reconciliation purposes.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The category of the individuals covered by the VADIR database encompasses veterans, service members, and their dependents. This would include current service members, separated service members, and their dependents; as well as veterans whose VA military service benefits have been sought by others (e.g., burial benefits).

CATEGORIES OF RECORDS IN THE SYSTEM: The record, or information contained in the record, may include identifying information (e.g., name, contact information, Social Security number), association to dependents, cross reference to other names used, military service participation and status information (branch of service, rank, enter

on duty date, release from active duty date, military occupations, type of duty, character of service, awards), reason and nature of active duty separation (completion of commitment, disability, hardship, etc.), combat/ environmental exposures (combat pay, combat awards, theater location), combat deployments (period of deployment, location/country), Guard/ Reserve activations (period of activation, type of activation), military casualty/disabilities (line of duty death, physical examination board status, serious/very serious injury status, DoD rated disabilities), education benefit participation, eligibility and usage, healthcare benefit periods of eligibility (TRICARE, CHAMPVA), and VA compensation (rating, Dependency and Indemnity Compensation (DIC), award amount).

RECORD SOURCE CATEGORIES: Information in this system of records is provided by components of the Department of Defense.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

1. Department of Defense: VA may disclose the record of an individual included in this system to DoD systems or offices for use in connection with matters relating to one of DoD's programs to enable delivery of healthcare or other DoD benefits to eligible beneficiaries.
2. Department of Defense Manpower Data Center (DMDC): VA may disclose the name, address, VA file number, effective date of compensation or pension, current and historical benefit pay amounts for compensation or pension, service information, date of birth, competency payment status, incarceration status, and social security number of veterans and their surviving spouses to the Department of Defense Manpower Data Center (DMDC) to reconcile the amount and/or waiver of service, department and retired pay.

3. Department of Defense Enrollment Eligibility Reporting System (DEERS): VA may disclose the name, address, VA file number, date of birth, date of death, social security number, and service information to DoD. DoD will use this information to identify retired veterans and dependent members of their families who have entitlement to DoD benefits but who are not identified in the Department of Defense Enrollment Eligibility Reporting System (DEERS) program and to assist in determining eligibility for Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) benefits. This purpose is consistent with 38 U.S.C. 5701.

4. Federal Agencies, for Research: VA may disclose information to a Federal agency for the purpose of conducting research and data analysis to perform a statutory purpose of that Federal agency upon the prior written request of that agency.

5. Law Enforcement: VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

6. DoJ for Litigation or Administrative Proceeding: VA may disclose information to the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her individual capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

7. Nonprofits, for RONA: To a nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits under title 38, provided that the disclosure is limited the names and addresses of present or former members of the armed services or their beneficiaries, the records will not be used for any purpose other than that stated in the request, and the organization is aware of the penalty provision of 38 U.S.C. 5701(f).

8. Contractors: VA may disclose information to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

9. Data breach response and remediation, for VA: VA may disclose information to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records, (2) VA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

10. Data breach response and remediation, for another Federal agency:

VA may disclose information to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed

breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

11. Congress: VA may disclose information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

12. NARA: VA may disclose information to the National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

13. Federal Agencies, for Computer Matches: VA may disclose information from this system to other Federal agencies in accordance with a computer matching program to determine or verify eligibility of veterans receiving VA benefits or medical care under title 38.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are transmitted between DMDC and VA over a dedicated telecommunications circuit using approved encryption technologies. Records (or information contained in records) are maintained in electronic format in the VADIR Oracle database. These records cannot be directly accessed by any VA employee or other users. Information from VADIR is disseminated in three ways: (1) Approved VA systems electronically request and receive data from VADIR, (2) data is provided between VADIR and DMDC for reconciliation of records or to identify retired veterans and dependents who have entitlements to DoD benefits but are not identified in DEERS, and (3) periodic electronic data extracts of subsets of information contained in VADIR are provided to approved VA

offices/systems. Backups of VADIR data are created regularly and stored in a secure off-site facility.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Electronic files are retrieved using various unique identifiers belonging to the individual to whom the information pertains to include such identifiers as name, claim file number, social security number and date of birth.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are retained indefinitely until a records retention schedule is approved by the Archivist of the United States. The records control for the VDR system hardware and user logs is GRS 4.2: Information Access and Protection Records Item 130 located at <https://www.archives.gov/records-mgmt/grs.html>.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Physical Security: The primary VADIR system is located in the AITC and the backup disaster recovery system is located in the Philadelphia Information Technology Center at Philadelphia, PA. Access to data processing centers is generally restricted to center employees, custodial personnel, Federal Protective Service, and other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All other persons needing access to computer rooms are escorted.

System Security: Access to the VA network is protected by the usage of two factor authentication. Once on the VA network, two factor authentication is required to gain access to the VADIR server and/ or database. Access to the server and/or database is granted to only a limited number of system administrators and database administrators. In addition, VADIR has undergone assessment and authorization based on a risk assessment that followed National Institute of Standards and Technology Vulnerability and Threat Guidelines. The system is considered stable and operational and a final

Authority to Operate has been granted. The system was found to be operationally secure, with very few exceptions or recommendations for change.

RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. The VA regulations implementing the Privacy Act are at 38 C.F.R. 1.575-582.

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Additionally, to the extent that information contested is identified as data provided by DMDC, which is part of the Defense Logistics Agency (DLA), the DLA rules for accessing records, for contesting contents, and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Privacy Act Officer, Headquarters, Defense Logistics Agency, ATTN: DES-B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060-6221.

NOTIFICATION PROCEDURES: Generalized notice is provided by the publication of this notice. For specific notice, see Record Access Procedure, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 74 FR 37093 (July 27, 2009).

[FR Doc. 2022-27988 Filed: 12/22/2022 8:45 am; Publication Date: 12/23/2022]